

Amendment to the Drawings:

Please amend the drawings as described below, and as shown in the attached drawing sheets labeled "ANNOTATED SHEET" and "REPLACEMENT SHEET":

In Figure 1, insert reference numeral "104" to refer to the bus connecting elements 108, 112, 116, and 130, as shown.

### REMARKS

Reconsideration of this application, based on this amendment and these following remarks, is respectfully requested.

Claims 1, 3, 5 through 8, 11 through 13, and 17 through 24 remain in this case. Claims 1, 3, 5 through 8, 11 through 13, 17 through 22, and 24 are amended. Claims 2, 4, 9, 10, 14 through 16, and 25 through 37 are canceled.

The specification was objected to because of informalities in the Abstract. The Abstract is amended as suggested by the Examiner, to overcome the objection.

The specification and drawings were also objected because the "system bus 104" to which reference is made in the specification was not shown by a reference numeral in the drawings. Figure 1 is amended to include the reference to Figure 1, in a manner consistent with the cited portion of the specification. This amendment to Figure 1 is presented by way of an annotated marked-up drawing, and a replacement sheet of the drawings, both submitted with this Amendment. Applicants submit that no new matter is presented by this amendment to the drawings, and further submit that, upon entry of this amendment to Figure 1, the objection to the drawings and specification on this basis will be overcome.

Claims 6, 17 through 18, 25, 26, 29, and 30, and their dependent claims 19, 27, 28, and 31, were rejected under §112, ¶2, as indefinite for failing to particularly point out and distinctly claim the subject matter of the invention, by including the relative term "substantially". Remaining claims 6, 17, and 18 are amended to cancel the objectionable word, overcoming the rejection to those claims and to dependent claim 19. Reconsideration of this rejection in light of this amendment is respectfully requested.

Claims 1 through 24 were rejected under §102(e) as anticipated by the Jeong et al. reference<sup>1</sup>. Claims 1 through 37 were rejected under §102(b) as anticipated by the Jones et al. reference<sup>2</sup>.

Claims 25 through 37 were also rejected under §102(b) as anticipated by the Santon et al. reference<sup>3</sup>. Claims 25 through 37 are canceled to advance the prosecution of this case, obviating this grounds of rejection.

Claim 1 is amended to clarify its novelty and patentability over the applied prior art. Amended claim 1 is now directed to a method of accessing encrypted information stored in a flash memory storage device by operating a host system in communication with a reader, where the reader includes a memory storing a key according to which the information stored in the flash memory is encrypted. The claimed method now includes the step of inserting the flash memory storage device into the reader, forwarding an access code from the host system to the reader, and obtaining the key from the reader responsive to that access code being valid for the reader. The claimed method further requires decrypting the information stored on the flash memory storage device using the key, and forwarding the decrypted stored information to the host system.

Support for this amendment to claim 1 is clearly present in the specification.<sup>4</sup> As such, no new matter is presented by this amendment to claim 1.

Claims 2, 4, 9, and 10 are canceled in light of the amendment to claim 1, upon which they previously depended. Claims 3, 5 through 8, 11, and 12 are amended for consistency to amended claim 1, upon which they directly or indirectly depend.

The method of amended claim 1 provides important advantages over conventional secure flash memory systems. These advantages include the additional security of storing an encryption key on a reader, rather than on a host system, such that it is more difficult for an unauthorized

---

<sup>1</sup> U.S. Patent Application Publication No. 2002/0174351 A1, published November 21, 2002 on an application filed October 24, 2001 by Jeong et al.

<sup>2</sup> U.S. Patent No. 6,623,637, issued April 22, 1997 to Jones et al.

<sup>3</sup> U.S. Patent No. 5,058,162, issued October 15, 1991 to Santon et al.

<sup>4</sup> See, e.g., specification of S.N. 10/092,049, at page 15, line 27 through page 15, line 10.

user to obtain the key, and also more difficult to access the encrypted information in the flash memory without accessing the reader.<sup>5</sup>

Applicants respectfully submit that amended claim 1 and its dependent claims are novel over the applied references.

The Jeong et al. reference is directed to the securing of a host adapter that is connected between two buses in a computer system, in which one bus is connected to the central processing unit (CPU) of the system, and the other bus is connected to a storage device such as a hard disk.<sup>6</sup> Nowhere does the Jeong et al. reference anywhere disclose the inserting of a flash memory storage device into a reader, or decrypting information stored on the flash memory storage device using a key obtained from the reader. As such, the method of claim 1 is clearly novel over the Jeong et al. reference.

In addition, the Jeong et al. reference fails to otherwise disclose the method of amended claim 1, because it operates in a completely different fashion because of its intended use in connection with a hard disk drive. The reference discloses that its "host adapter" simply decrypts incoming data (either from the CPU or from the disk drive) according to one secret key, and encrypts outgoing data (to the disk drive or to the CPU, respectively) according to another secret key.<sup>7</sup> Nowhere does the Jeong et al. reference teach forwarding an access code from a host system to a reader, responsive to which a key is obtained and according to which the stored information is decrypted, as required by amended claim 1. Accordingly, Applicants submit that amended claim 1 and its dependent claims are novel over the Jeong et al. reference.

Applicants further respectfully submit that the amendment to claim 1 is also sufficient to overcome its rejection as anticipated by the Jones et al. reference. Specifically, the Jones et al. reference nowhere discloses the inserting of a flash memory device into a reader, nor the obtaining of the key for decrypting the contents of the flash memory device from the reader responsive to a valid access code from the reader. Rather, the Jones et al. reference is directed to

---

<sup>5</sup> Specification, *supra*, page 10, line 5 through page 11, line 4.

<sup>6</sup> Jeong et al., *supra*, paragraph [0012].

a password-protected PCMCIA card, in which the data in the common memory array (150) is effectively password protected.<sup>8</sup> But the common memory array (150) is nowhere separated from the PCMCIA card of the Jones et al. reference, however. And therefore, there is never any "inserting" of a flash memory storage device into a reader according to the Jones et al. reference, as required by amended claim 1.

This difference between the claimed method and the Jones et al. reference is substantial. The system of the Jones et al. reference suffers from the very problem addressed by the method of claim 1. As expressly stated by the Jones et al. reference itself, "the data stored in a protected partition within the memory card 100 is available only to those who possess both the card and the password".<sup>9</sup> In contrast, according to the method of claim 1, the possessor of the access code and of the flash memory storage device storing the encrypted data still cannot access the encrypted data; the reader containing the key is necessary for decryption.<sup>10</sup> Accordingly, the difference between the method of claim 1 and the teachings of the Jones et al. reference is much more significant than simply the step of inserting a flash memory storage device into a reader – rather, this inserting of the flash memory storage device into a reader and the obtaining of a key from the reader responsive to forwarding a valid access code from the host system results in a substantially more secure method of securing data.

For these reasons, Applicants submit that amended claim 1 and each of its dependent claims are novel over the Jeong et al. and Jones et al. references applied thereagainst.

Applicants further respectfully submit that there is no suggestion from the prior art, including from the Jeong et al. and Jones et al. references, and the Santon et al. reference applied against claim 25 *et seq.*, to modify these teachings in such a manner as to reach amended claim 1 and its dependent claims.

---

<sup>7</sup> Jeong et al., *supra*, paragraphs [0034] and [0035].

<sup>8</sup> Jones et al., *supra*, column 7, line 61 through column 8, line 46.

<sup>9</sup> Jones et al., *supra*, column 8, lines 35 through 37.

<sup>10</sup> Specification, *supra*, page 10, line 25 through page 11, line 4.

This lack of suggestion is apparent considering the wide difference in the nature of the data storage systems between those of the prior art references and those of amended method claim 1. As mentioned above, the Jeong et al. reference is directed to securing data on a hard disk drive, and the Jones et al. reference is directed to providing a secure PCMCIA card, without involving a reader. The Santon et al. reference is directed to unlocking software from a ROM disk, for example a compact laser disk.<sup>11</sup> As such, none of these references are directed to the accessing of encrypted data on a flash memory storage device that is insertable into a reader, as required by claim 1.

And this difference between the applied references and the method of amended claim 1 results in substantial differences in the overall operating methods involved. As mentioned above, the Jeong et al. reference does not forward an access code from the host system to a reader, and obtain a key for decrypting the data responsive to the access code being valid; rather, the Jeong et al. reference performs a decrypt/encrypt sequence on data going in either direction, in effect changing the encryption key from that of the CPU to that of the disk drive. And, as mentioned above relative to the Jones et al. reference, its method of operating suffers from the very problem addressed by the invention of amended claim 1, because its storage array is never separated from the remainder of the PCMCIA card. Accordingly, Applicants submit that amended claim 1 and its dependent claims are not only novel but are patentably distinct over the references of record in this case.

Independent apparatus claim 13 is similarly amended to overcome the rejection. The system of amended claim 13 now requires a host system, a flash memory reader coupled to the host system, and means for decrypting information stored on a flash memory device received at the interface of the flash memory reader, using a key that is stored in reader memory and that is obtained by circuitry in the reader responsive to a valid access code received from the host system. For the reasons discussed above relative to amended claim 1, Applicants submit that no new matter is presented by this amendment, and that the system of amended claim 13 provides similar advantages as the method of amended claim 1 discussed above.

---

<sup>11</sup> Santon et al., *supra*, column 5, lines 9 through 13.

Claims 14 through 16 are canceled, considering the amendment to claim 13. Claims 17 through 22 and 24 are amended, for consistency with the amendment to claim 13; upon which they depend.

Applicants submit that amended claim 13 and its dependent claims are novel over the Jeong et al. and Jones et al. references applied thereagainst.

The Jeong et al. reference nowhere discloses an interface in a flash memory reader for receiving a flash memory storage device, nor does it disclose any means for decrypting information stored on the flash memory storage device using a key obtained from the reader. These differences between the reference and the claims are emphasized by considering the context of the Jeong et al. reference in securing a hard disk drive in a computer system, and also the manner in which the Jeong et al. performs its functions. Specifically, the system of the Jeong et al. reference includes a "host adapter" that decrypts incoming data according to one secret key, and encrypts outgoing data according to another secret key.<sup>12</sup> The host adapter of the Jeong et al. reference does not receive an access code from a host system, nor does it obtain a key from that access code, with the key used in eventually decrypting the stored information, as results in the system of amended claim 13.

Referring to the Jones et al. reference, nowhere does that reference disclose an interface in a reader for receiving a flash memory storage device, nor does it disclose any means for the obtaining of a key for decrypting the contents of the flash memory device from the reader responsive to receiving a valid access code from the host system. Rather, the common memory array of the Jones et al. reference is never removed from or received by an interface in the reader. As such, the system of the Jones et al. reference suffers from the very problem addressed by the invention of claim 13, in that the protected data is never separated from the reader. In the system of amended claim 13, on the other hand, because the reader has an interface for receiving a flash memory storage device, an unauthorized possessor of the access code and of the flash memory storage device storing the encrypted data cannot access the encrypted data, because it is the

---

<sup>12</sup> Jeong et al., *supra*, paragraphs [0034] and [0035].

reader that has a reader memory storing the key that is used in decryption.<sup>13</sup> For these reasons, Applicants submit that the teachings of the Jones et al. reference also fall short of the requirements of amended claim 13.

For these reasons, Applicants submit that amended claim 13 and its dependent claims are all novel over the Jeong et al. and Jones et al. references applied thereagainst.

Nor is there suggestion to modify the teachings of these references in such a manner as to reach amended claim 13, or its dependent claims. As discussed above, neither the Jeong et al. nor the Jones et al. references are directed to a flash memory system, including a flash memory reader with an interface for receiving a flash memory storage device, to which claim 13 is directed. Because of this, and also because of the resulting substantial differences in the construction of the systems disclosed in those references and considering that the references suffer from the very problem addressed and solved by the system of amended claim 13, Applicants submit that amended claim 13 and its dependent claims are not only novel but are patentably distinct over the references of record in this case.

The prior art cited as pertinent but not applied has been considered, but is not felt to come within the scope of the claims in this case.

---

<sup>13</sup> Specification, *supra*, page 10, line 25 through page 11, line 4.



For these reasons, Applicants respectfully submit that all claims now in this case are in condition for allowance. Reconsideration of this application is therefore respectfully requested.

Respectfully submitted,



Rodney M. Anderson

Registry No. 31,939

Attorney for Applicants

Anderson, Levine & Lintel, L.L.P.

14785 Preston Road, Suite 650

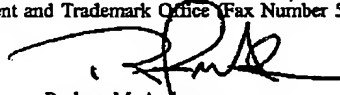
Dallas, Texas 75254

(972) 664-9554

CERTIFICATE OF FACSIMILE TRANSMISSION

37 C.F.R. 1.8

The undersigned hereby certifies that this correspondence is being facsimile transmitted to the Patent and Trademark Office (Fax Number 571.273.8300) on March 1, 2006.



Rodney M. Anderson  
Registry No. 31,939

## ANNOTATED SHEET

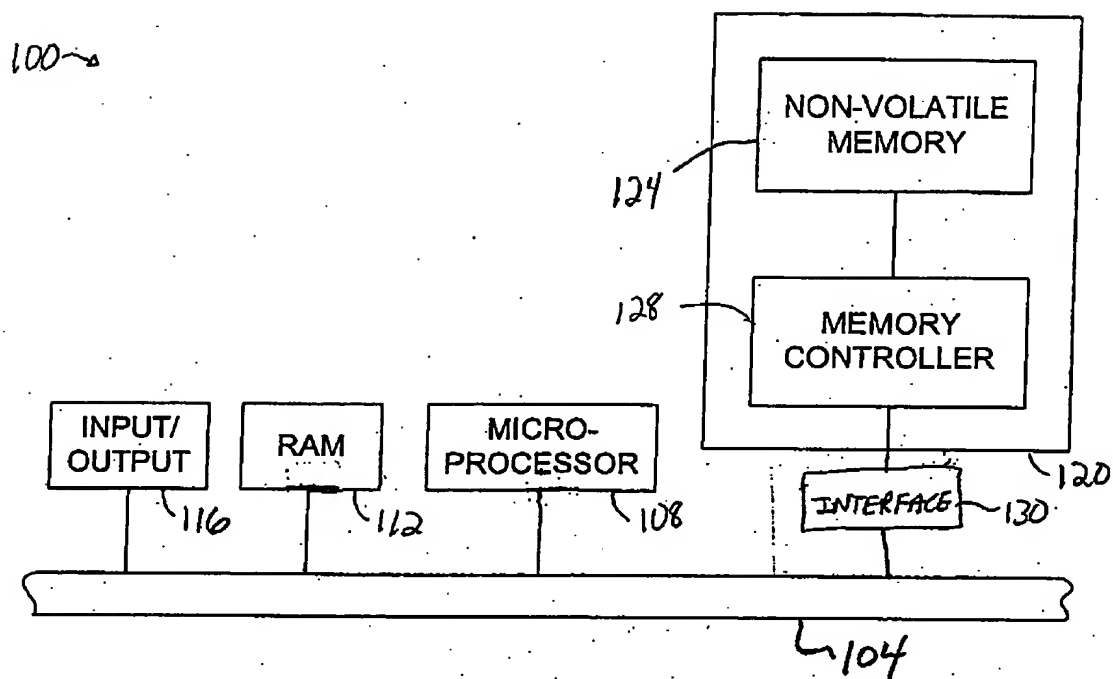


Fig. 1

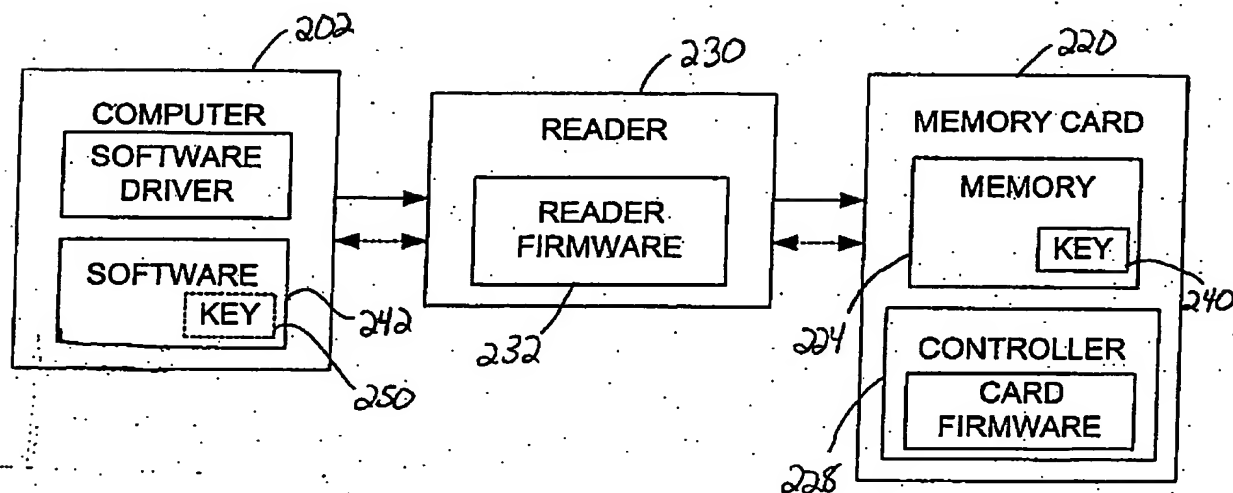


Fig. 2